BHBIA Data Analytics Guidelines
Data Protection – Rights of Data Subjects

These guidelines are part of a series designed to provide guidance on the legal and ethical issues impacting data analysts

INTRODUCTION

Data Protection

The 'Data Subject' is the person whom particular personal data is about. Data Analytics practitioners may handle healthcare professional's data, perhaps from a secondary research exercise or a commercial database e.g. a doctor list used for segmentation or targeting exercises. It therefore pays to be aware of the General Data Protection Regulation (GDPR)/Data Protection Act (DPA) 2018 implications. The GDPR/DPA 2018 says that data subjects' have the following data protection rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling (e.g. use of AI techniques).

Privacy

Under the UK Data Protection Act 2018, and the European Convention on Human Rights states "*everyone has the right to respect for his private and family life, his home and his correspondence*."

In addition, individuals that are involved in market research (primary or secondary) as respondents (e.g. interviewees) or contributors (e.g. through passive digital listening) have the right to remain anonymous and have their input remain confidential. This is a basic and critical market research tenet.

So individuals from whom data is collected must be offered anonymity (their identity will not be revealed) and confidentiality (their identity will not be linked to their input). They can choose to waive these rights but for market research they must be offered them.

MORE DETAIL UPON DATA PROTECTION RIGHTS FOR DATA SUBJECTS

To be informed

The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice (email or website typically).

To be informed it must include:

- ✓ **Name of the organisation/individual** seeking consent and their **contact details,** if this is not the data controller you must identify the data controller
- ✓ **Name any third parties who will rely on the consent i.e. any recipients of the personal data** (naming the type of organisation is not sufficient) e.g. the name of the commissioning client if they are to be given access to non-anonymised recordings to respondents participating in market research (MR)
- ✓ **Legal basis for processing** some business processes may rely on "legitimate interest" whereas others (like automated profiling) may require specific consent
- ✓ **Purposes** of the processing – why you want the data
- ✓ **Types of processing activity** – what you will do with the data
- ✓ **Where processing is based** and **details of any data transfer to countries without adequate data protection** (generally countries outside the European Union - EU)
- ✓ **How long the data will be stored** or if that's not possible, the criteria used to decide this
- ✓ **Right to withdraw consent** at any point and other rights - to have their personal data rectified or erased, to access or move their data, to restrict or object to data processing in future and to complain to the data protection authority (the Information Commissioner's Office in the UK) - some of this detail could be put into the privacy notice. It must be as easy to withdraw consent as it was to give it, so it should be an easily accessible single step. It is good practice to tell individuals how to withdraw (including on the privacy notice).
- ✓ **Existence of any automated decision making** and its consequences
- ✓ **Contact details of data protection officer**

In addition, when the data is not obtained directly from the individual, the data subject must also be informed of:

- ✓ The **categories** of personal data to be collected
- ✓ The **source** of the personal data

- **To access data**
  The reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

- **To rectification**
  Individuals are entitled to have personal data rectified if it is inaccurate or incomplete (within 1 month).

- **To erasure**
  The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances e.g. when the individual withdraws consent If an individual has asked not to be contacted you must keep or have access to a 'do not contact' list or database to make sure you don't contact them.

- **To restrict processing**
  Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future. If an individual asks not to be contacted for the purpose of market research they are exercising their right to restrict processing (not their right to erasure). It is important not to confuse the two different rights. Quite clearly if you are going to observe a request not to be contacted for the purposes of market research you will need to store some personal data to do this.

- **To data portability**
  This allows individuals to obtain and reuse their personal data for their own purposes across different services, it allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

- **To object to processing**
  Individuals have the right to object to (amongst other things) processing based on legitimate interests.

- **Not to be subject to automated decision-making including profiling**
  Individuals have the right not to be subject to a decision when it is based on automated processing; and it produces a legal effect or a similarly significant effect on the individual.

Remember - if in doubt, be as specific as you can be on why you're handling the data. Your Legal department may suggest a Privacy Impact Assessment (PIA) of any secondary data projects to ascertain the right legal basis for processing the data.

For further information see:

The Information Commissioner's Office website
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

The BHBIA's website
https://www.bhbia.org.uk/guidelines/gdprupdates.aspx

This guidance is provided by the BHBIA for information purposes only and is not intended and should not be construed as regulatory or legal advice. It does not cover all legislative and regulatory requirements pertaining to Members and it is the responsibility of all Members to familiarise themselves with these.

The Guidelines are provided by the Data Analytics Guidelines Team within the BHBIA's Ethics & Compliance Committee.

Jason Bryant, Data Analytics Team Lead
Darren Kottler, Data Analytics Team
Klaas Breukel, Data Analytics Team
Catherine Ayland, BHBIA Ethics Advisor

If you have any queries about these Guidelines, please visit www.bhbia.org.uk and submit your query via 'My BHBIA' dashboard. Please note: this ad hoc advisory service is available to full BHBIA members only.

British Healthcare Business Intelligence Association
Ground Floor, 4 Victoria Square, St. Albans, Herts AL1 3TF
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk

A Private Limited Company Registered in England and Wales